Lucas-Lehmer Primality Test

D. Cortild (s4279239) and A. Villegas Sanabria (s4368908)

University of Groningen, February 2, 2022

***Abstract*—Primality testing is a rather complicated and computationally heavy process. For special numbers, such as Mersenne numbers, more specific and lighter methods exist. One of them is the Lucas-Lehmer primality test, which will be discussed throughout this article.**

***Index Terms*—Lucas-Lehmer, Primality test, Prime numbers, Mersenne primes**

I. Introduction

The *Great Internet Mersenne Prime Search* (GIMPS) is the result of a collaborative effort by volunteers using free software to find Mersenne primes. Since its foundation in 1996 by George Woltman up until today, the project has discovered a total of 17 primes, most of them being the largest known prime at the time of their discovery. The largest Mersenne prime number the project has found is $2^{82589933} - 1$, which was discovered in late 2018. The main algorithm on which the GIMPS project builds is the Lucas-Lehmer primality test, as it is an efficient way of testing for Mersenne primes, and that it can be run efficiently on modern binary computer architectures.

The Lucas-Lehmer test (LLT) is a primality test for Mersenne numbers $M_p := 2^p - 1$, with p an odd prime. It relies on the following sequence $(s_i)_{i\in\mathbb{N}}$

$$s_i = \begin{cases} 4 & \text{if } i = 0 \\ s_{i-1}^2 - 2 & \text{else} \end{cases}$$

The first terms of the sequence are $4, 14, 194, 37634$ and 1416317954, a more exhaustive list can be found in sequence A003010 on OEIS.
The LLT then states that M_p, for p an odd prime, is prime if and only it divides s_{p-2}. As an example, $M_5 = 2^5 - 1 = 31$ is prime since 31 divides $s_3 = 37634 = 31 \cdot 1214$. On the other hand, one may test computationally that s_9 is not divisible by $M_{11} = 2047$, predicated by the known non-primality of $2047 = 23 \cdot 89$.

The principal aim of this paper is to prove the validity, study the effectiveness and explore different variations of this test. To start, in section II, we prove several results about quadratic residues, which will be used throughout the proofs in later sections. A reader familiar with the notions of quadratic residues can skip this section, as it is mainly covering the basics. In section III we perform a preliminary analysis on the sequence $(s_i)_{i\in\mathbb{N}}$ and different Mersenne numbers. Sections IV and V are devoted to proving respectively the necessity and the sufficiency of the LLT. Throughout the last section, section VI, an implementation of the test and its time complexity will be studied.

II. Quadratic Residues

Throughout the proof of the validity of the Lucas-Lehmer Test, we will use different results about perfect squares modulo p, or what is better known as quadratic residues modulo p. Although originally developed for a purely mathematical pleasure, they nowadays play a role in acoustics, cryptography, graph theory and primality testing. This section is devoted to the introduction of some notions and to the proofs of the claims resulting from them. Most knowledge exposed here is often assumed prior knowledge, and is included in this article for the sake of completeness. A reader familiar with the notion of quadratic residues and their results might find it useful to move on to section III.

The main part of the early results in this section are inspired by the results in *Reciprocity Laws: From Euler to Eisenstein* by Franz Lemmermeyer ([6]) and by the works of O. Baumgart in *Über das Quadratische Reciprozitätsgesetz* ([1]).

Definition. Let p be an odd prime number and a an integer. We say a is a *quadratic residue* modulo p if it is congruent to a perfect square modulo p. Else a is said to be a *quadratic non-residue* modulo p.

In order to perform mathematical operations with quadratic residues, we define a mathematical symbol, the Legendre Symbol, which indicates whether a certain number is a quadratic residue modulo p or not.

Definition. Take p an odd prime and a an integer non-multiple of p. The Legendre symbol is defined as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}$$

Additionally, if a is a multiple of p, we denote $\left(\frac{a}{p}\right) = 0$.

One big property of the Legendre Symbol, known as Euler's Criterion, is that it may be written as a closed formula depending on a and p only. This will simplify several calculations later. The result follows from the definition of the Legendre Symbol and Lemma 2.5 of [8].

Proposition 1 (Euler's Criterion)**.** Let p be an odd prime and a an integer. Then it holds that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Using this proposition, we may prove that the Legendre symbol is multiplicative with respect to the first input.

Corollary 2. Let p be an odd prime and a, b integers. Then

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Proof. By Proposition 1,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

Since both the left most and right most expressions are in $\{-1, 0, 1\}$ and $p \geq 3$, we conclude that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

□

Although Euler's Criterion gives a pretty good formula for the Legendre symbol and heavily simplifies the computations, computation $a^{\frac{p-1}{2}}$ is not always the best way to go, and is not always feasible. Gauss's Lemma, presented next, gives a much more reliable method to compute any Legendre symbol.

Lemma 3 (Gauss's Lemma)**.** Let p be an odd prime and a an integer coprime to p. Consider the half-system modulo p,

$$A = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$$

And let n be the number of values $k \in A$ such that $ka \pmod{p} \notin A$. Then

$$\left(\frac{a}{p}\right) = (-1)^n$$

Proof. Denote by $B \subset A$ the set of elements $k \in A$ such that $ka \pmod{p} \notin A$. By definition, $n = |B|$.
Denote by σ the map

$$\sigma : A \to A, \quad k \mapsto \pm ak \pmod{p}$$

Where the $\pm$ is chosen such that $\pm ak \pmod{p} \in A$. This is always possible since ak is non-zero modulo p and

$$\mathbb{F}_p^\times = \{k \mid k \in A\} \bigcup \{-k \mid k \in A\}$$

Also, the sign of $\pm$ is uniquely defined as either $ak \pmod{p} \in A$ or $-ak \pmod{p} \in A$, but not both. Also, observe that if $k \in B$, then the sign is $-$ and else the sign is $+$.
Note that σ is an injection, since, for $k, r \in A$

$$\sigma(k) = \sigma(r) \iff \pm ak \equiv ar \pmod{p}$$
$$\iff \pm k \equiv r \pmod{p} \iff k = r$$

Hence σ is a permutation of A.

We may thus compute the following value

$$\begin{aligned} a^{\frac{p-1}{2}} \prod_{k \in A} k &\equiv \prod_{k \in A} ak \\ &\equiv \prod_{k \in A} \pm\sigma(k) \\ &\equiv (-1)^{|B|} \prod_{k \in A} \sigma(k) \\ &\equiv (-1)^n \prod_{k \in A} k \pmod{p} \end{aligned}$$

And hence

$$\implies \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n$$

As wanted. □

Gauss's Lemma will allow us to prove more general results later on, but firstly we will find an easy formula for the quantity $\left(\frac{2}{p}\right)$.

Corollary 4. Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \not\equiv \pm 1 \pmod{8} \end{cases}$$

Proof. Consider the numbers

$$2, 4, \dots, 2\left\lfloor \frac{p}{4} \right\rfloor, 2\left\lceil \frac{p}{4} \right\rceil, \dots, p-1$$

Since p is odd, the middle values are distinct. By Gauss's Lemma, we pick n to be the number of values in this sequence with residue modulo p in the range $[p/2, p-1]$. These are exactly the numbers

$$2\left\lceil \frac{p}{4} \right\rceil, \dots, p-1$$

And thus

$$n = \frac{p-1}{2} - \left\lceil \frac{p}{4} \right\rceil + 1$$

We thus conclude that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{2} - \left\lceil \frac{p}{4} \right\rceil} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \not\equiv \pm 1 \pmod{8} \end{cases}$$

□

Another consequence of Gauss's Lemma is Eisenstein's Lemma, which gives a more convenient way of expressing the value n and thus a simpler way of expressing the Legendre symbol. Although Gauss's Lemma gave us an easier expression for whether a number is a quadratic residue or not, it is still not perfect and is rather hard to compute. The following lemma will simplify yet again that expression.

Lemma 5 (Eisenstein's Lemma)**.** Let p be an odd prime and a an integer coprime to p. Consider the value

$$n = \sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2ak}{p} \right\rfloor$$

Then

$$\left(\frac{a}{p}\right) = (-1)^n$$

Proof. Using Lemma 3, it is clear we need to prove the two definitions of n yield the same result, thus proving that they have the same parity. Using the notation of the proof of the previous lemma, we shall prove that $k \in \boldsymbol{B}$ if and only if $\left\lfloor \frac{2ak}{p} \right\rfloor$ is odd. Then n according to the definition of this statement would be of the same parity as $|\boldsymbol{B}|$, the n of the previous statement, and the values of $(-1)^n$ would thus coincide for both values of n, concluding the proof.

Observe that $k \in \boldsymbol{B}$ if for some integer value α,

$$\alpha p + \frac{p}{2} < ak < \alpha p + p \iff \left\lfloor \frac{2ak}{p} \right\rfloor = 2\alpha + 1$$

On the other hand, $k \notin \boldsymbol{B}$ is for some integer value α,

$$\alpha p < ak < \alpha p + \frac{p}{2} \iff \left\lfloor \frac{2ak}{p} \right\rfloor = 2\alpha$$

This conclude the proof. □

The very closed formula for $\left(\frac{a}{p}\right)$ given in Eisenstein's Lemma allows us to prove a very important result of Quadratic Residues, namely the Law of Quadratic Reciprocity. The proof is presented via a geometric argument, inspired by Eisenstein's proof presented in *Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem*, by Reinhard C. Laubenbacher and David J. Pengelley ([7]).

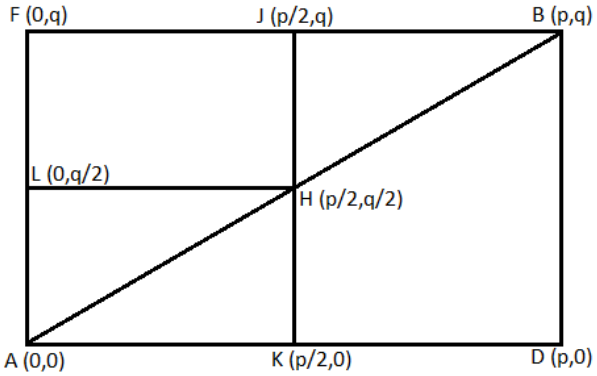
Theorem 6 (Law of Quadratic Reciprocity)**.** Let p and q be distinct odd prime numbers. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Proof. We shall use Eisenstein's Lemma to prove the result. Indeed, translated into sums, the Law is equivalent to proving that

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{2pk}{q} \right\rfloor \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod 2$$

We prove the result using the following diagram. The coordinates of the points may be read of it and one might observe that The line passing through $\boldsymbol{A}, \boldsymbol{H}$ and $\boldsymbol{B}$ has a slope of q/p.



Denote by O_Δ, E_Δ and T_Δ the total number of integer points with odd, even or any x coordinate strictly in the figure Δ.

Observe that no integer point (n, m) may lie on the segment $\boldsymbol{AB}$ strictly between $\boldsymbol{A}$ and $\boldsymbol{B}$, since that would imply

$$pm = qn \implies p|qn \implies p|n \implies p \leq |n|$$

Contradicting that the point (n, m) is on the inside of the segment $\boldsymbol{AB}$.

Now the quantity $\left\lfloor \frac{2qk}{p} \right\rfloor$ represents the number of integer points $(2k, \alpha)$, where $0 < \alpha \leq 2k \cdot q/p$. Since equality may never occur, this is the number of integer points with x coordinate $2k$ strictly inside the triangle $\boldsymbol{ABD}$. So

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2qk}{p} \right\rfloor = E_{ABD}$$

Next observe that each integer column (fixed value of x) has exactly $q-1$, an even number, integer points strictly inside the rectangle $\boldsymbol{AFBD}$. In specific, the number of integer points with an even x coordinate in the rectangle $\boldsymbol{AFBD}$ is even. In other terms,

$$E_{AFBD} \equiv 0 \pmod 2$$

Since no integer points lie on $\boldsymbol{AB}$, we thus observe that

$$E_{AFBD} = E_{BDKH} + E_{BHJ} \implies E_{BDKH} \equiv E_{BHJ} \pmod 2$$

Then we consider the transformation $(x, y) \mapsto (p-x, q-y)$, which is basically a rotation by 180° through the centre of the rectangle $\boldsymbol{H}$. This transformation maps in a bijective manner an integer point to an integer point. Also observe that the triangle $\boldsymbol{BHJ}$ is mapped to the triangle $\boldsymbol{AHK}$, and that an even x coordinate integer point is mapped to an odd x coordinate integer point. In more mathematical terms, this yields

$$O_{AHK} = E_{BHJ}$$

Since no integer point lies on the vertical line with x coordinate $p/2$, we learn

$$E_{ABD} \equiv E_{AHK} + E_{BDKH} \equiv E_{AHK} + E_{BHJ}$$

$$\equiv E_{AHK} + O_{AHK} \equiv T_{AHK} \pmod 2$$

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2qk}{p} \right\rfloor \equiv T_{AHK} \pmod 2$$

Analogously,

$$\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{2pk}{q} \right\rfloor \equiv T_{AHL} \pmod 2$$

Since no points may lie on the hypotenuse of the triangle, this translates to

$$\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{2qk}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{2pk}{q} \right\rfloor \equiv T_{AKHL} \pmod 2$$

But the number of points strictly in that rectangle is

$$\frac{p-1}{2}\frac{q-1}{2}$$

Just as wanted. □

Now that we have all the tools in hand to easily compute any Legendre symbol, we might want to determine whether or not 3 and 6 are quadratic residues and under which conditions. These two results will be the main building blocks of the proof of the necessity of the Lucas-Lehmer Test, Theorem 18.

Lemma 7. Let $p > 3$ be an odd prime. Then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \not\equiv \pm 1 \pmod{12} \end{cases}$$

Proof. Since both 3 and p are odd distinct primes, we may use the Law of Quadratic Reciprocity, Theorem 6, in order to obtain

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

Since the quadratic residues modulo 3 are 0 and 1, and that p cannot be 0 modulo 3, we know that

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

And thus

$$\left(\frac{3}{p}\right) = \begin{cases} (-1)^{\frac{p-1}{2}} & \text{if } p \equiv 1 \pmod 3 \\ (-1)^{\frac{p+1}{2}} & \text{if } p \equiv 2 \pmod 3 \end{cases}$$

Which simplifies to

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \not\equiv \pm 1 \pmod{12} \end{cases}$$

□

The computation of $\left(\frac{6}{p}\right)$ is a direct consequence of Corollaries 2 and 4 and Lemma 7.

Lemma 8. Let $p > 3$ be an odd prime. Then

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24} \\ -1 & \text{if } p \not\equiv \pm 1, \pm 5 \pmod{24} \end{cases}$$

Proof. Using the multiplicativity of the Legendre symbol, we conclude that

$$\left(\frac{6}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{2}{p}\right)$$

The rest follows from Corollary 4 and Lemma 7. □

On a different note, quadratic residues may be used to study the number of solutions to a quadratic equation. In Lemmas 9 and 11 we study such equations in respectively one and two variables.

Lemma 9. Let p be an odd prime and a be an integer. The number of solutions $x \in \mathbb{Z}/p\mathbb{Z}$ of

$$x^2 \equiv a \pmod p$$

is exactly $1 + \left(\frac{a}{p}\right)$.

Proof. Firstly, observe that if $a = 0$, then the equation $x^2 \equiv 0 \pmod p$ has a unique solution $x \equiv 0 \pmod p$, so the formula is also verified.

Additionally, if a is a quadratic non-residue modulo p, then the solution obviously has no solutions and thus the formula is verified.

If a is a non-zero quadratic residue modulo p, then the equation has at least one solution, call it x. Notice that $-x$ will also be a solution, and it is distinct from x since

$$x \equiv -x \pmod p \implies 2x \equiv 0 \pmod p$$

Since p is odd, 2 is invertible, and thus we would have $x \equiv 0 \pmod p$. This contradicts the fact that $a \not\equiv 0 \pmod p$. Hence, the equation has at least 2 solutions. Suppose the equation has a third solution $y \not\equiv \pm x \pmod p$. Then

$$x^2 \equiv a \equiv y^2 \pmod p$$

$$\implies p \mid (x-y)(x+y)$$

$$\implies y \equiv x \pmod p \quad \text{or} \quad y \equiv -x \pmod p$$

Both contradict the assumptions about y, so no third solution to the equation may exist. So in this case the equation has exactly 2 solutions, hence verifying the formula. □

In order to extend this result to a quadratic equation in two variables, we first need to compute the sum of all Legendre symbols for a fixed p.

Lemma 10. Let p be an odd prime. Then

$$\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = 0$$

Proof. First we prove that the number of elements $a \in \mathbb{F}_p^\times$ such that $\left(\frac{a}{p}\right) = 1$ is exactly $\frac{p-1}{2}$. Consider the map

$$f : \mathbb{F}_p^\times \to \mathbb{F}_p^\times, x \mapsto x^2$$

This map is a homomorphism since

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$$

By the Homomorphism Theorem (Theorem VIII.2.1 of [5]),

$$\mathbb{F}_p^\times / \ker(f) \cong f(\mathbb{F}_q^\times)$$

By definition of f, $\ker(f)$ is the set of solutions to $x^2 = 1$ in $\mathbb{F}_p^\times$. By Corollary 9, this equation has exactly 2 solutions in $\mathbb{F}_p^\times$, as $\left(\frac{1}{p}\right) = 1$. Thus $|\ker(f)| = 2$, and hence

$$|f(\mathbb{F}_p^\times)| = \frac{|\mathbb{F}_p^\times|}{|\ker(f)|} = \frac{p-1}{2}$$

Thus exactly $\frac{p-1}{2}$ elements of $\mathbb{F}_p^\times$ are quadratic residues modulo p, as wanted.

In other words, $\left(\frac{a}{p}\right) = 1$ for exactly half of the elements in $\mathbb{F}_p^\times$, and thus $\left(\frac{a}{p}\right) = -1$ for the other half. Additionally, by definition, $\left(\frac{0}{p}\right) = 0$. Thus, we deduce

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

As wanted. □

We may now relate the number of solutions to a quadratic equation to a function of the Legendre symbol of its coefficients.

Lemma 11. Let p be an odd prime and $\alpha, \beta \in \mathbb{F}_p^\times$. The number of solutions $(x, y) \in \mathbb{F}_p^2$ of

$$\alpha x^2 + \beta y^2 \equiv 1 \pmod{p}$$

is exactly $p - \left(\frac{-\alpha\beta}{p}\right)$.

Proof. Denote by $N(\cdot)$ the number of solutions to the equation $\cdot$ in $\mathbb{F}_p$. We are looking for the quantity

$$N \coloneqq N(\alpha x^2 + \beta y^2 = 1)$$

Observe that, by Lemma 9,

$$\begin{aligned} N &= \sum_{\alpha a + \beta b = 1} N(x^2 = a) N(y^2 = b) \\ &= \sum_{\alpha a + \beta b = 1} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right) \\ &= \sum_{\alpha a + \beta b = 1} 1 + \left(\frac{a}{p}\right) + \left(\frac{b}{p}\right) + \left(\frac{ab}{p}\right) \end{aligned}$$

Observe that the following map is a bijection.

$$\mathbb{F}_p \to \{(a, b) : \alpha a + \beta b = 1\}, a \mapsto (a, \beta^{-1}(1 - \alpha a))$$

By this bijection, and by Lemma 10,

$$\sum_{\alpha a + \beta b = 1} \left(\frac{a}{p}\right) = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = 0$$

Analogously,

$$\sum_{\alpha a + \beta b = 1} \left(\frac{b}{p}\right) = 0$$

So the wanted expression is, using Corollary 2,

$$\begin{aligned} N &= p + \sum_{a \in \mathbb{F}_p} \left(\frac{ab}{p}\right) \\ &= p + \sum_{a \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \\ &= p + \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a\beta^{-1}(1 - \alpha a)}{p}\right) \\ &= p + \left(\frac{\beta^{-1}}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)\left(\frac{1 - \alpha a}{p}\right) \\ &= p + \left(\frac{\beta}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a^{-1}}{p}\right)\left(\frac{1 - \alpha a}{p}\right) \\ &= p + \left(\frac{\beta}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a^{-1} - \alpha}{p}\right) \end{aligned}$$

Where we used the equality $\left(\frac{x^{-1}}{p}\right) = \left(\frac{x}{p}\right)$, following from the fact that

$$\left(\frac{x}{p}\right)\left(\frac{x^{-1}}{p}\right) = \left(\frac{xx^{-1}}{p}\right) = \left(\frac{1}{p}\right) = 1$$

And that

$$\left(\frac{x}{p}\right) \in \{-1, 1\}$$

Notice that $a \mapsto a^{-1} - \alpha$ is a bijection from $\mathbb{F}_p^\times$ to $\mathbb{F}_p \backslash \{-\alpha\}$. Thus the wanted expression is

$$\begin{aligned} N &= p + \left(\frac{\beta}{p}\right) \sum_{a \in \mathbb{F}_p \backslash \{-\alpha\}} \left(\frac{a}{p}\right) \\ &= p + \left(\frac{\beta}{p}\right)\left[-\left(\frac{-\alpha}{p}\right) + \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right)\right] \\ &= p - \left(\frac{\beta}{p}\right)\left(\frac{-\alpha}{p}\right) \\ &= p - \left(\frac{-\alpha\beta}{p}\right) \end{aligned}$$

As wanted. □

The study of quadratic residues is of course much more exhaustive, but we will limit ourselves to these interesting results. The main results that will be used throughout the following sections are Lemmas 7, 8 and 11.

III. Preliminary Analysis

We start by formalizing the result we want to prove under the form of a theorem.

Theorem 12 (Lucas-Lehmer Primality Test)**.** Define $(s_i)_{i\in\mathbb{N}}$ as $s_0 = 4$ and $s_i = s_{i-1}^2 - 2$ for $i \geq 1$. Then, for an odd prime p, the Mersenne number $M_p \coloneqq 2^p - 1$ is prime if and only if it divides s_{p-2}.

One might wonder why this test is enough to test the primality of every Mersenne number since it is only valid for odd primes, but in fact most Mersenne numbers are trivially non-prime.

Claim 13. If the Mersenne number M_p is prime, then p is prime.

Proof. We shall prove this statement by contraposition. So we want to prove that p not prime implies M_p not prime. The first case to analyse is $p = 1$, which in turn yields $M_p = M_1 = 1$, which is not prime.

Now assume that $p = qr$, $q, r > 1$, is a composite number. Then we know that

$$M_r = 2^r - 1 \Big| 2^{qr} - 1 = M_p$$

Since $1 < M_r < M_p$, we conclude that M_p is composite, concluding the proof. □

A Mersenne number M_p can thus only be prime if p is prime. If additionally p is even, then $p = 2$, and it is easily verifiable. Else p is an odd prime, and Theorem 12 applies. The test thus produces a full characterization of all Mersenne primes, if one disregards the case $p = 2$.

The recurrence relation in Theorem 12 is not particularly inviting. Its non-linear nature also means that it might not even be solvable. Luckily, in this case it is, using a well-motivated initial guess.

Lemma 14. Let s_0 be fixed. Suppose there exists an invertible real 2×2 matrix ω such that $\omega + \omega^{-1} = s_0 I_2$, where I_2 is the 2×2 identity matrix.

Then the integer recurrence relation $s_{i+1} = s_i^2 - 2$ for $i \geq 1$ with s_0 fixed is solved by

$$s_n I_2 = \omega^{2^n} + \omega^{-2^n}$$

Proof. Suppose $\omega \in \mathbb{R}^{2\times 2}$ is invertible and solves

$$\omega + \omega^{-1} = s_0 I_2$$

Then $n = 0$ clearly verifies the formula. Suppose some non-negative integer n does so too. Then

$$\begin{aligned}
s_{n+1} I_2 &= (s_n^2 - 2) I_2 \\
&= s_n^2 I_2 - 2 I_2 \\
&= \left(s_n I_2\right)^2 - 2 I_2 \\
&= \left(\omega^{2^n} + \omega^{-2^n}\right)^2 - 2 I_2 \\
&= \left(\omega^{2^n} + \omega^{-2^n}\right)^2 - 2 I_2 \\
&= \omega^{2^{n+1}} + \omega^{-2^{n+1}} + 2 \cdot \omega^{2^n} \cdot \omega^{-2^n} - 2 I_2 \\
&= \omega^{2^{n+1}} + \omega^{-2^{n+1}}
\end{aligned}$$

So $n + 1$ also verifies the formula, and by the principle of mathematical induction it holds for all non-negative integers, and the given equation solves the recurrence. □

From this, we may directly deduce the general solution to the sequence $(s_i)_{i\in\mathbb{N}}$ used in Theorem 12.

Corollary 15. The recurrence relation $s_{i+1} = s_i^2 - 2$ for $i \geq 1$ with $s_0 = 4$ is solved by

$$s_n I_2 = \omega^{2^n} + \omega^{-2^n}$$

Where

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \omega = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$$

Proof. By Lemma 14, it is sufficient to prove that ω is invertible and that it satisfies $\omega + \omega^{-1} = s_0 I_2$. Both are verified since

$$\omega = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$$

And

$$\omega + \omega^{-1} = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} + \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$$

□

Having a more general and suitable formula for the terms in the sequence $(s_i)_{i\in\mathbb{N}}$ will allow us to prove both directions of Theorem 12 over the next two sections.

IV. Sufficiency of LLT

We formulate the sufficiency of the LLT as the first direction of Theorem 12 as follows

Theorem 16 (Sufficiency of LLT)**.** Define $(s_i)_{i\in\mathbb{N}}$ as $s_0 = 4$ and $s_i = s_{i-1}^2 - 2$ for $i \geq 1$. Then, for an odd prime p, if the Mersenne number $M_p \coloneqq 2^p - 1$ divides s_{p-2}, then it is prime.

We shall proceed by contradiction, assuming the division holds without M_p being prime. To reach this conclusion, we shall introduce a group and compute two different contradictory bounds for its size.

Claim 17. By $\mathbb{G}_n$ we denote the set

$$\mathbb{G}_n \coloneqq \left\{ \begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in (\mathbb{Z}/n\mathbb{Z})^{2\times 2} \ : \ a^2 - 3b^2 \equiv 1 \pmod{n} \right\}$$

With the binary multiplication $\cdot : \mathbb{G}_n \times \mathbb{G}_n \to \mathbb{G}_n$ inherited from the standard matrix multiplication modulo n.
The set $\mathbb{G}_n$ associated with the set operation $\cdot$ forms a group.

Proof. Firstly, observe that the set operation $\cdot$ is well-defined and closed in $\mathbb{G}_n$, as

$$\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 3d & c \end{pmatrix} = \begin{pmatrix} ac + 3bd & ad + bc \\ 3ad + 3bc & ac + 3bd \end{pmatrix}$$

The later is an element of $\mathbb{G}_n$ as

$$(ac+3bd)^2 - 3(ad+bc)^2 = (a^2-3b^2)(c^2-3d^2) \equiv 1 \pmod{n}$$

To prove that $\mathbb{G}_n$ is a group, it needs to verify the following three axioms:

- It is associative. Indeed, the set operation is standard matrix multiplication modulo n, which is associative so the restriction to $\mathbb{G}_n$ is so too.
- It has an identity element. Indeed, it is easily verified that $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an element of $\mathbb{G}_n$, and since it is an identity element to the standard matrix multiplication modulo n, it also is one to the restriction to $\mathbb{G}_n$.
- Each element has an inverse element. Indeed, if $\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \in \mathbb{G}_n$, then $\begin{pmatrix} a & -b \\ -3b & a \end{pmatrix}$ forms a right and left inverse, and is also contained in $\mathbb{G}_n$.

All axioms are thus verified, which concludes that $(\mathbb{G}_n, \cdot)$ forms a group. □

Now we are ready to prove Theorem 16, the sufficiency of the Lucas-Lehmer Test.

Proof. Suppose that M_p has a proper prime divisor $1 < q < M_p$. Notice that $q \neq 2$ since M_p is odd. Additionally, since p is odd, $M_p \equiv 2^p - 1 \equiv 1 \pmod 3$ so $q \neq 3$.

Observe that since s_{p-2} is a multiple of M_p, there exists an integer k such that

$$kM_p = s_{p-2} \implies kM_pI_2 = s_{p-2}I_2 = \omega^{2^{p-2}} + \omega^{-2^{p-2}}$$
$$\implies \omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - I_2$$

Since M_p is a multiple of q, the right-hand side is equal to $-I_2$ in $\mathbb{G}_q$, where $\mathbb{G}_q$ is defined as in Claim 17. Hence,

$$\omega^{2^{p-1}} = -I_2 \quad \text{and} \quad \omega^{2^p} = I_2$$

Notice that ω is in $\mathbb{G}_q$, so the order of ω in $\mathbb{G}_q$ divides 2^p, but not 2^{p-1}, and hence

$$\operatorname{ord}_{\mathbb{G}_q}(\omega) = 2^p$$

By Lagrange's theorem, this means that 2^p divides the order of $\mathbb{G}_q$, or in weaker terms,

$$2^p \leq \operatorname{ord}(\mathbb{G}_q)$$

On the other hand, observe that

$$\operatorname{ord}(\mathbb{G}_q) = \#\{(a,b) \in \mathbb{F}_q^2 \ : \ a^2 - 3b^2 \equiv 1 \pmod{q}\}$$

However, by Lemma 9, this set has at most $q+1$ elements. Thus, we conclude that

$$2^p \leq \operatorname{ord}(\mathbb{G}_q) \leq q + 1 < 2^p - 1 + 1 = 2^p$$

Which is obviously a contradiction. Hence, M_p has no proper divisor, so M_p is prime. □

One might notice that this proof could have been made easier by taking q to be the smallest proper divisor of M_p, forcing $q^2 < 2^p$, and altering the restriction of a determinant to be equal to 1 in Claim 17 to simply forcing a non-zero determinant. This however does not generalize, which is why we opted for this alternative proof.

This proves that whenever the divisibility holds, the primality holds. On a computational level, this is all we need. However, in order to make sure this will find all Mersenne primes, the divisibility is also necessary for the primality to hold. This is the necessity of the test, discussed in the next section.

V. Necessity of LLT

The necessity of the LLT may be formulated as the second direction of Theorem 12, as follows

Theorem 18 (Necessity of LLT)**.** Define $(s_i)_{i\in\mathbb{N}}$ as $s_0 = 4$ and $s_i = s_{i-1}^2 - 2$ for $i \geq 1$. Then, for an odd prime p, if the Mersenne number $M_p \coloneqq 2^p - 1$ is prime, then it divides s_{p-2}.

To prove this Theorem, we shall extract 2 key properties of a Mersenne primes, whose proof has been mainly covered earlier.

Claim 19. Let p be an odd prime. Then

$$\left(\frac{3}{M_p}\right) = -1 = \left(\frac{6}{M_p}\right)$$

Proof. By Lemmas 7 and 8, it is sufficient to prove that

$$M_p \equiv 7 \pmod{12} \quad \text{and} \quad M_p \equiv 7 \pmod{24}$$

Notice that the latter automatically implies the first, so we shall simply prove that

$$M_p \equiv 7 \pmod{24}$$

This is easily proven by induction on p, by replacing the assumption that p is an odd prime by the slightly stronger assumption that p is an odd integer ≥ 3. □

Claim 20. Let p be an odd prime and let A and B be 2×2 matrices with values in F_p such that $AB = BA$. Then

$$(A+B)^p \equiv A^p + B^p \pmod{p}$$

Proof. First notice that for $0 < k < p$, we have

$$\binom{p}{k} \equiv 0 \pmod{p}$$

Indeed, recall the definition of the binomial coefficient

$$\binom{p}{k} = \frac{p!}{k!\cdot(p-k)!}$$

Since $k, p-k < p$ and p is a prime, we know

$$p \nmid k! \quad \text{and} \quad p \nmid (p-k)!$$

But $p \mid p!$, and $\binom{p}{k}$ is an integer, hence

$$p \;\Big|\; \binom{p}{k}$$

As stated.

Now we shall prove the Binomial Theorem for commuting matrices. We claim the following formula holds

$$(A+B)^n = \sum_{i=0}^{n} \binom{n}{i} A^i B^{n-i}$$

It is clearly true for $n = 0$, which constitutes our base case. Suppose it is true for some integer value $n \geq 0$. Then

$$\begin{aligned}
(A+B)^{n+1} &= (A+B)(A+B)^n \\
&= \sum_{i=0}^{n} \binom{n}{i} A^{i+1} B^{n-i} + \sum_{i=0}^{n} \binom{n}{i} A^i B^{n-i+1} \\
&= \sum_{i=0}^{n+1} \binom{n}{i-1} A^i B^{n+1-i} + \sum_{i=0}^{n+1} \binom{n}{i} A^i B^{n+1-i} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} A^i B^{n+1-i}
\end{aligned}$$

So the formula also holds for $n+1$, so it holds for all integer values of n.

Combining the 2 previous observations thus yields that

$$(A+B)^p = \sum_{i=0}^{p} \binom{p}{i} A^i B^{p-i} \equiv A^p + B^p \pmod{p}$$

As wanted. □

We have now armed ourselves with enough tools to prove Theorem 18. This proof is inspired, although largely simplified, by a similar proof by Paul Garrett in [4].

Proof. Denote

$$\sigma := \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix}$$

Then it is easy to check that

$$\omega \equiv 6^{-1}\sigma^2 \pmod{M_p}$$

And thus by Claim 19

$$\begin{aligned}
\omega^{2^{p-1}} \equiv \omega^{\frac{M_p+1}{2}} &\equiv 6^{-1} \cdot \left(6^{\frac{M_p-1}{2}}\right)^{-1} \sigma^{M_p+1} \pmod{M_p} \\
&\equiv -6^{-1} \cdot \sigma^{M_p+1} \pmod{M_p}
\end{aligned}$$

Now notice that

$$\sigma = \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$$

The later two matrices commute, since the first is a diagonal matrix. Thus, we may apply Claim 19, Claim 20 and Fermat's Theorem to obtain

$$\begin{aligned}
\sigma^{M_p} &\equiv \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}^{M_p} + \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}^{M_p} \\
&\equiv \begin{pmatrix} 3^{M_p} & 0 \\ 0 & 3^{M_p} \end{pmatrix} + \left(\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}^2\right)^{\frac{M_p-1}{2}} \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&\equiv \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}^{\frac{M_p-1}{2}} \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&\equiv \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} 3^{\frac{M_p-1}{2}} & 0 \\ 0 & 3^{\frac{M_p-1}{2}} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&\equiv \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&\equiv \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \\
&\equiv \begin{pmatrix} 3 & -1 \\ -3 & 3 \end{pmatrix} \pmod{M_p}
\end{aligned}$$

And thus

$$\begin{aligned}
\omega^{2^{p-1}} &\equiv -6^{-1} \cdot \sigma^{M_p+1} \\
&\equiv -6^{-1} \cdot \begin{pmatrix} 3 & -1 \\ -3 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 3 & 3 \end{pmatrix} \\
&\equiv -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \equiv -I_2 \pmod{M_p}
\end{aligned}$$

And thus, finally,

$$\begin{aligned}
-I_2 \equiv \omega^{2^{p-1}} \equiv \omega^{2^{p-2}} \cdot \omega^{2^{p-2}} \pmod{M_p} \\
\implies \omega^{2^{p-2}} + \omega^{-2^{p-2}} \equiv 0 \pmod{M_p} \\
\implies s_{p-2} \equiv 0 \pmod{M_p}
\end{aligned}$$

As wanted originally. □

This finalizes the proof of the equivalence between the divisibility conditions and the primality condition of the Lucas-Lehmer Test (Theorem 12).

VI. Time Complexity

As described throughout the sections, the Lucas-Lehmer Test is actually a rather simple test to execute. It merely consists of computing values of a sequence and testing for a divisibility criterion at the end. Since the recurrence is of order 1, it is unnecessary to store more than one previous value at a time, causing the test to be memory friendly too. The following Python script shows one possible implementation of the Lucas-Lehmer Test.

```
def LLT(p):
    Mp = 2**p - 1
    s = 4
    for i in range(p-2):
        s = (s*s - 2) % Mp
    if s == 0:
        return "PRIME"
    else:
        return "COMPOSITE"
```

One might observe that all values of the sequence (s_i) are taken modulo M_p in the code, as it significantly reduces the size of the values and makes the algorithm much faster without adapting it too much. It also avoids the otherwise inevitable memory overflow problems.

Observe that the final test for divisibility takes constant time with respect to p, as it only check whether the final value is 0 or not. Computing M_p in the very start requires $\approx \log(p)$ operations, if done efficiently, by multiply-and-square method. Also, each step of the algorithm consists of 4 operations. In total, the algorithm thus runs in $O(p)$ operations.

However, it is unrealistic to consider the operation -2 to have the same complexity as the operation $s \cdot s$, especially for large values of s. Instead, we will consider the number of *bit-level operations*. In these calculations, we assume we are working on a modern binary computer, allowing us to do certain tricks. This discussion is partially inspired, although highly remodelled, from *Integer multiplication in time O(n log n)* by David Harvey, Joris van der Hoeven ([3]) and from *Cunningham numbers in modular arithmetic* by E. V. Zima and A. M. Stewart ([9]).

For starter, the number $M_p = 2^p - 1$ lives on p bits, in fact we know it is the p-bit string of all ones. Evaluating and storing M_p thus runs in $O(p)$ bit operations.

Since s is always taken modulo M_p we know that s lives on p bits. Using the naive multiplication method one is taught in elementary school makes the multiplication $s \cdot s$ cost $O(p^2)$ bit operations. More efficient multiplication algorithms exist, such as Fürer's Algorithm, however we shall restrict us to the naive approach at the time.

Another quite heavy operation is the modulo M_p. A naive approach would be subtracting M_p until the number is smaller than M_p. Given that $s \cdot s$ might be as large as M_p^2, this approach might require M_p subtractions, amounting to a total of $O(pM_p) = O(p2^p)$ bit operations to simply get the value of $s \cdot s - 2$ modulo M_p. A much more efficient way is to observe that

$$\alpha \equiv \lfloor \alpha / 2^p \rfloor + (\alpha \mod 2^p) \pmod{2^p - 1}$$

This may be seen by writing

$$\alpha = 2^p \cdot \beta + \gamma, \quad \beta \in \mathbb{N}, \gamma \in [0, 2^p - 1]$$

Where $\beta = \lfloor \alpha / 2^p \rfloor$ and $\gamma = (\alpha \mod 2^p)$.
Since $s^2 - 2$ lives on $2p$ bits, the first term represent the first p bits of $s^2 - 2$, and the second term the other p bits. Reducing $s^2 - 2$ modulo M_p is thus a simple question of a p-bit addition. Notice that the sum might be larger than M_p, but never larger than $2M_p$, so the total number of bit operations is $O(p)$.

Every iteration of the algorithm thus runs in $O(p^2)$ bit operations. The entire algorithm thus runs in $O(p^3)$ bit operations, so we may conclude the Lucas-Lehmer Test evaluates whether $2^p - 1$ is a prime in polynomial time $O(p^3)$ in p.

References

[1] O. Baumgart. "Über das Quadratische Reciprozitätsgesetz". In: *Zeitschrift für Mathematik und Physik* 30 (1885), pp. 169–277.

[2] J. W. Bruce. "A Really Trivial Proof of the Lucas-Lehmer Test". In: *The American Mathematical Monthly* 100.4 (1993), pp. 370–371.

[3] Joris van der Hoeven David Harvey. *Integer multiplication in time O(n log n)*. Annals of Mathematics, Princeton University, Department of Mathematics. 2020.

[4] Paul Garrett. *Lucas-Lehmer criterion for primality of Mersenne numbers*. 2010.

[5] J.S. Müller Jaap Top. *Group Theory*. University of Groningen. 2018.

[6] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein*. Springer, 2000.

[7] David J. Pengelley Reinhard C. Laubenbacher. "Eisenstein's Misunderstood Geometric Proof of the Quadratic Reciprocity Theorem". In: *College Mathematics Journal* 25 (1994), pp. 29–34.

[8] Jaap Top. *Security and Codes: Part II - Security*. University of Groningen. 2015.

[9] E. V. Zima and A. M. Stewart. "Cunningham numbers in modular arithmetic". In: *Programming and Computer Software* 33 (Mar. 2007), pp. 80–86.